ALLEN & OVERY

Crisis Management – Cybercrime

allenovery.com

Cybercrime – Reducing risks through prevention and response

Cybercrime – criminal activities that exploit electronic infrastructures – is one of the greatest threats faced by companies in the digital age. Both the number of attempted attacks and the level of professionalism employed by the perpetrators have been on the rise for years. Attacks are thus occurring more often while also becoming more complex.

The size of a company and its area of activity are entirely irrelevant in this context. Cybercrime is not limited to large corporates or particular business fields. And with increasing numbers of employees working from home, new windows of opportunity are opening up for cybercriminals.

At the same time, cybercrime knows no national borders. It is a global problem – in terms of both its origins and its effects.

Cybercrime can take many different forms, and can equally have manifold consequences. At present, numerous cases are being seen where people are lured into divulging information or transferring money following a dishonest misrepresentation of facts (CEO fraud). Attacks whereby loopholes in IT systems are exploited and the data contained on them encrypted before a ransom demand is issued (ransomware) are similarly common.

The resulting damage takes many forms:

First and foremost, companies lose money as a result of unwarranted transfers or **ransom payments**. But other consequences of a cyberattack, such as the **loss of key data**, **business interruptions** or **reputational damage**, can be just as damaging. Moreover, **sanctions** may also be imposed if, for instance, the loss of data was the result of errors committed by the company itself or the company failed to properly fulfil its duties in the event of a cyberattack. These may include both duties relating to the protection of certain data and reporting duties in the event of a data loss, for instance.

It is thus imperative that companies take real steps to address the risk presented by cybercrime. They should take preventative measures to reduce the risk of falling victim to cybercriminals. And companies that have been targeted by a cyberattack should respond quickly and in a targeted manner in order to limit the damage suffered by the company as far as possible.

From our perspective, cases of cybercrime are thus to be viewed as corporate crises requiring a fast and legally sound response. We can offer our experience in the relevant legal fields, combined with our contacts at the competent authorities and other service providers. As a legal firm with a global network, we are in a position to process matters quickly and effectively, even across several jurisdictions.

Be it prevention or response, cybercrime requires your attention. We would be happy to advise you – please don't hesitate to contact us.

Possible actions

In order to reduce the likelihood of falling victim to cybercrime, companies should at least consider taking the following preventative measures:

- Increase risk awareness – sensitise staff to potential risks
- Introduce and regularly update policies for handling of data and computers/mobile phones
- Implement an emergency/response plan (incl. relevant contacts)
- Constantly monitor and review the levels of protection on IT infrastructure
- Conduct a risk analysis
- Clarify the legal framework relating to cybercrime
- Consider taking out relevant insurance

If your company has fallen victim to cybercrime, immediate and targeted action – depending on the individual case – is key:

- Where IT systems have been targeted: review systems, identify scope of attack, restore data from backup where necessary/possible, gather evidence
- Where payments have been made: take initial measures to stop the cashflow (in third countries where necessary
- If a ransom is being demanded: examine legality and weigh up pros and cons of payment
- Review reporting duties
- Evaluate cooperation with the authorities
- Explore own and potential third-party claims under civil law relating to the attack
- Implement communication strategy
- Draw conclusions from the attack; improve systems where necessary

We have wide-ranging experience in all these fields, as well as the pertinent third-party contacts. We would be pleased to act as central contact, not only advising you and your company in advance, but also providing valuable support in crisis situations.

Cybercrime as a crisis – our approach

Holistic approach

We want to act as a central contact, supporting our clients in times of crisis. All relevant fields can either be covered internally or we can provide the relevant contacts to third parties, such as IT service providers or authorities. With just one call to us, you will receive all the support you need – quickly and reliably.

Experts in all fields

Cybercrime requires advice on various aspects. In terms of general preparation, compliance is key in order to reduce the probability of falling victim to an attack. In a crisis situation, advice is required in particular in the fields of corporate law (in particular advising managing directors on how to manage the crisis), data protection law (in particular reporting duties and observing data protection regulations), media/publication law (in particular communication strategies with staff and the public), white-collar crime (in particular questions of culpability and contact with authorities), insurance law (in particular disputes with potential insurers), banking & finance (in particular questions of financial feasibility where ransom demands have been made), investigations (in particular investigating the incident in order to eliminate weaknesses), litigation (in particular asserting own claims and defending against third-party claims) and employment law (in particular potential action against employees).

Our experts have comprehensive experience in all of these fields. We, as immediate IT Incident Reponse, also have the requisite contacts at third-party providers.

Global network

Cybercrime knows no national boundaries. The perpetrators are often located abroad and money is frequently quickly withdrawn from Germany before being transferred elsewhere. Thanks to our global network, we can rapidly ensure that the necessary action is taken in other jurisdictions, too. Thus, money can in some cases be recovered or offenders more effectively pursued through cooperation with local authorities.

Moreover, in a globalised environment, sanctions in other jurisdictions may have to be observed in the context of cybercrime. The US Office of Foreign Assets Control (OFAC), for instance, published a note in September 2021 threatening harsh sanctions for companies that are seen to have facilitated cybercrime.

Our expertise

Advising a large shipping company

in connection with a cybercrime incident and the related payment of USD 2 million. We were able to stop payment of half of the money in another country and recover it for our client. At the same time, we prepared criminal proceedings, worked together with domestic and foreign authorities to identify the perpetrators and asserted claims under domestic and foreign civil law. The criminal proceedings have already been launched and we are currently exploring claims under civil law.

Advising a listed fashion company

in connection with a cybercrime incident and related payments of several hundred thousand euro to an account in Hong Kong. We were able to stop a significant portion of the erroneous payments and help our client to recover the stopped amounts via a court in Hong Kong.

Advising a major online trading company

in advance of its planned IPO on questions relating to the prevention of cybercrime and IT security.

Advising listed companies

on reporting duties under corporate and capital markets law relating to cybercrime and ransomware attacks.

Advising a Middle Eastern corporate group

following a cyberattack on the core systems of one of its largest European industrial subsidiaries, including contacting the public prosecutor and press communication.

Supporting a leading German real estate company

on preparing a response plan for cyberattacks and responding to several data protection breaches, including notifying German and UK data protection authorities and communicating with the individuals involved.

Advising on management board duties of information

to the supervisory board in the context of cybercrime and ransomware attacks.

Supporting an energy company

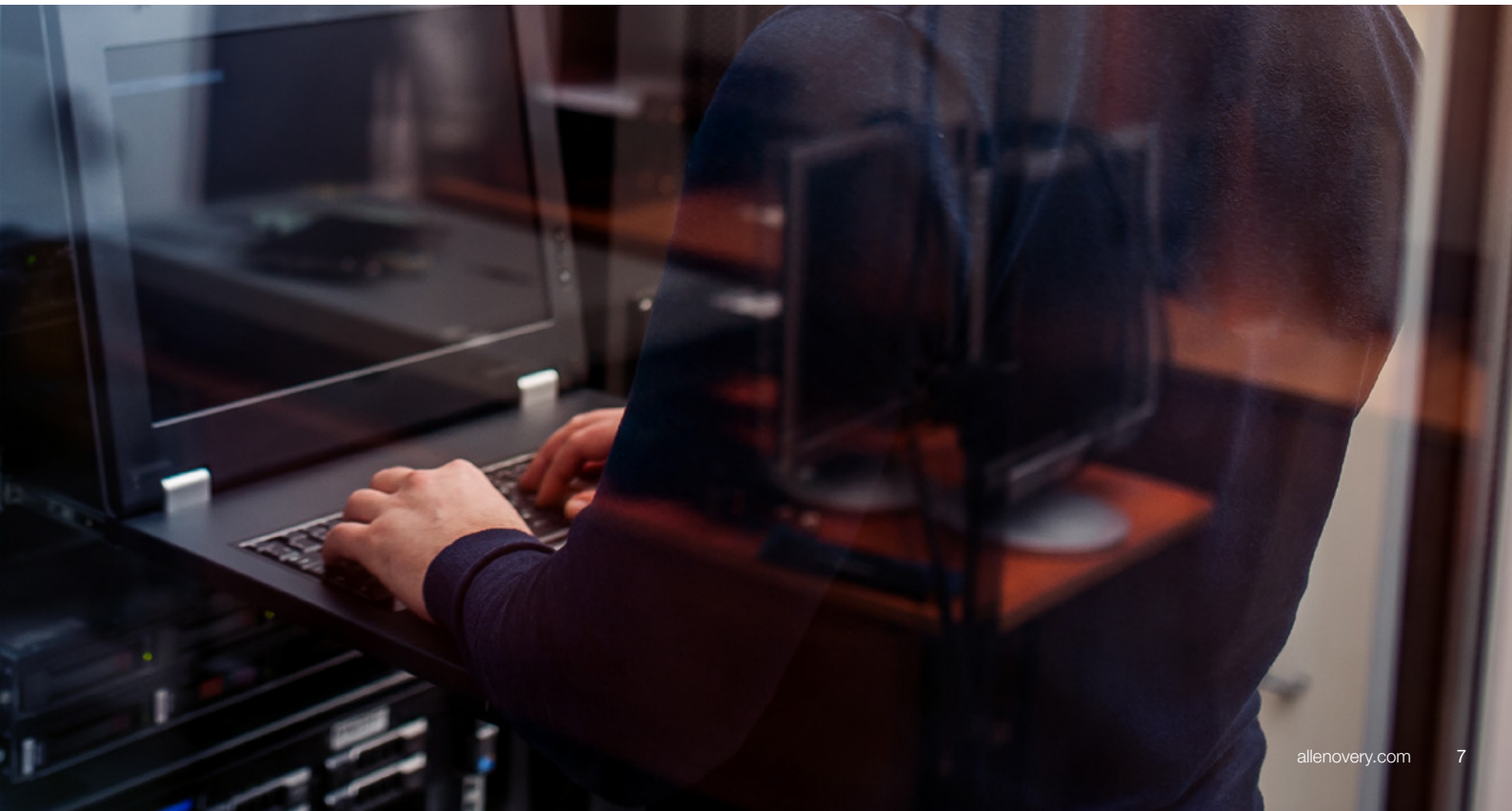
in the wake of a case of CEO fraud.

Advising various companies

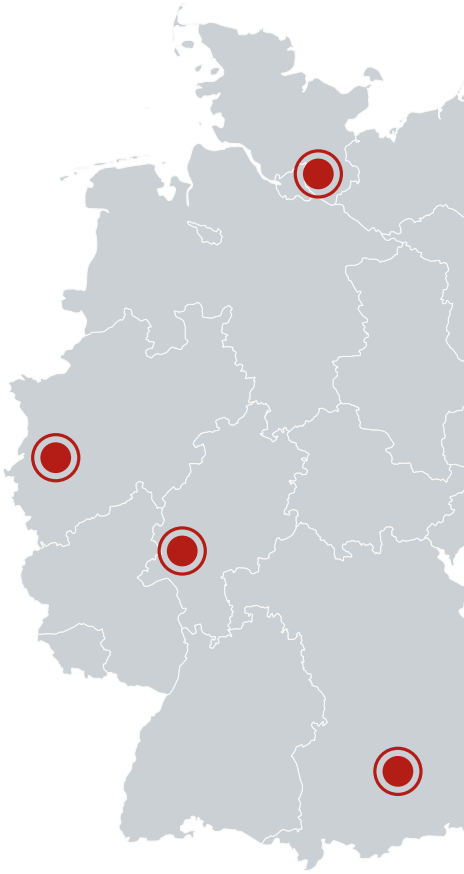
on prevention measures under corporate law against various external attacks, including in cyberspace.

Advising an international health technology company

in connection with a data protection breach relating to health data, including negotiations with data protection authorities and court proceedings.



Allen & Overy Germany



General information

4 Offices

420 Employees

220 Lawyers

Sectors

- Automotive
- Public sector
- Real estate
- Financial services
- Energy
- Life Sciences & Healthcare
- Private Equity
- Telecommunications, Media & Technology
- Infrastructure & Transportation

Principal areas of advice include

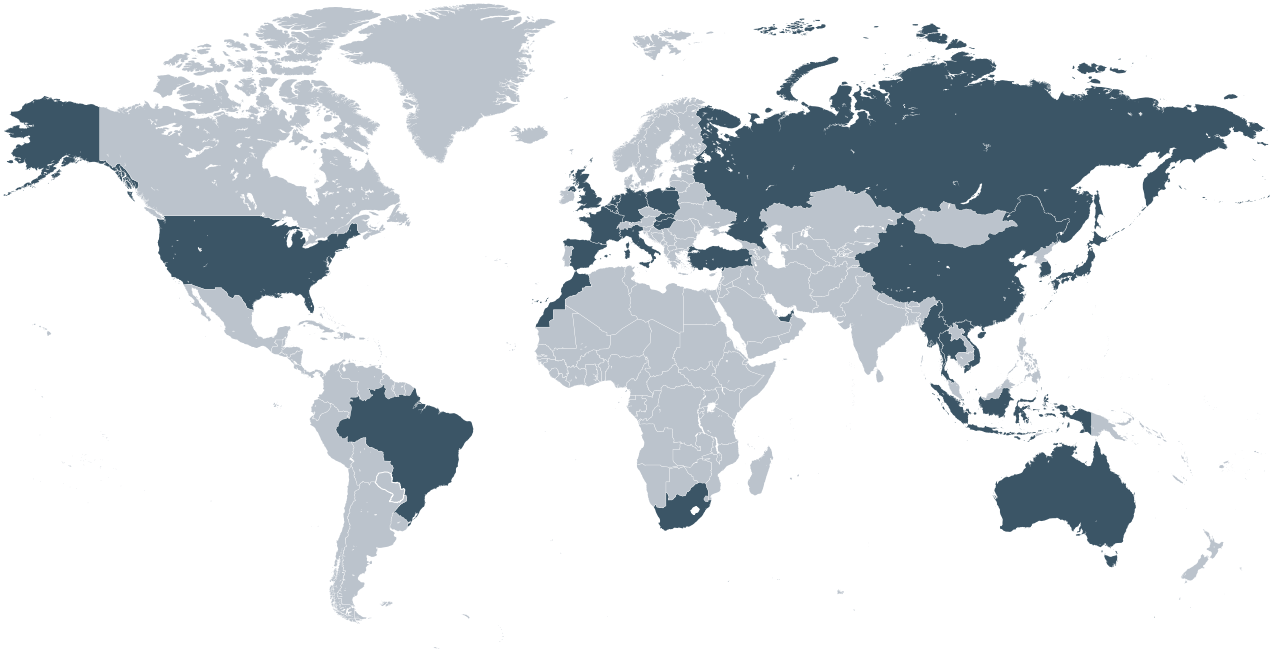
- Employment law
- Commercial legal protection
- Restructuring
- Banking & Finance
- Capital markets
- Tax & insolvency
- Corporate Governance public and Compliance
- Antitrust law
- Procurement law/Public law
- Corporate/M&A
- Insurance corporate law

Allen & Overy worldwide

Allen & Overy is one of the largest and most widely branched international commercial law firms in the world, with around **580 partners** and **5,600 employees**. It is important for us to offer legal advice on site and according to local conditions. Thanks to our international network with **40 locations** on **five continents**, we are represented at the locations where our clients are also active. In this way, we guarantee local advice and at the same time can fall back on an almost seamless network for cross-border mandates. Where we are not represented with our own offices, we have an established network of partner law firms.

International Law Firm of the Year

IFLR 2021



North America

Los Angeles
New York
Silicon Valley
Washington, D.C.

Central & South America

São Paulo

* Associated office

Europe

Amsterdam
Antwerp
Belfast
Bratislava
Brussels
Budapest
Düsseldorf
Frankfurt
Hamburg
Istanbul
London
Luxembourg
Madrid
Milan
Moscow
Munich
Paris
Prague
Rome
Warsaw

Africa

Casablanca
Johannesburg

Middle East

Abu Dhabi
Dubai

Asia Pacific

Bangkok
Beijing
Hanoi
Ho Chi Minh City
Hong Kong
Jakarta*
Perth
Seoul
Shanghai
Singapore
Sydney
Tokyo
Yangon

Cyber Crime contacts

Jens Matthes
Partner – Duesseldorf
Tel +49 211 2806 7121
jens.matthes@allenovery.com

Michael Weiss
Partner – Frankfurt
Tel +49 69 2648 5453
michael.weiss@allenovery.com

Erik Windthorst
Partner – Frankfurt
Tel +49 69 2648 5583
erik.windthorst@allenovery.com

Tim Mueller
Counsel – Frankfurt
Tel +49 69 2648 5996
tim.mueller@allenovery.com

Achim Schmid
Counsel – Duesseldorf
Tel +49 211 2806 7221
achim.schmid@allenovery.com

David Schmid
Counsel – Frankfurt
Tel +49 69 2648 5774
david.schmid@allenovery.com

Sebastian Schulz
Counsel – Frankfurt
Tel +49 69 2648 5915
sebastian.schulz@allenovery.com

Andre Wandt
Counsel – Frankfurt
Tel +49 69 2648 5684
andre.wandt@allenovery.com

Catharina Glugla
Senior Associate – Duesseldorf
Tel +49 211 2806 7103
catharina.glugla@allenovery.com

Veronika Gaile
Associate – Frankfurt
Tel +49 69 2648 5481
veronika.gaile@allenovery.com

Niklas Haas
Associate – Frankfurt
Tel +49 69 2648 5950
niklas.haas@allenovery.com

Jasmin Hense
Associate – Frankfurt
Tel +49 69 2648 5444
jasmin.hense@allenovery.com

Laura Jung
Associate – Frankfurt
Tel +49 69 2648 5858
laura.jung@allenovery.com

Global presence

Allen & Overy is an international legal practice with approximately 5,600 people, including some 580 partners, working in more than 40 offices worldwide. A current list of Allen & Overy offices is available at www.allenovery.com/global_coverage.

Allen & Overy means Allen & Overy LLP and/or its affiliated undertakings. Allen & Overy LLP is a limited liability partnership registered in England and Wales with registered number OC306763. Allen & Overy LLP is authorised and regulated by the Solicitors Regulation Authority of England and Wales.

The term partner is used to refer to a member of Allen & Overy LLP or an employee or consultant with equivalent standing and qualifications or an individual with equivalent status in one of Allen & Overy LLP's affiliated undertakings. A list of the members of Allen & Overy LLP and of the non-members who are designated as partners is open to inspection at our registered office at One Bishops Square, London E1 6AD.

ROW
CS2112_CDD-67144_ADD-99467